AMENDMENTS TO THE CLAIMS:

This listing of the claims will replace all prior versions, and listings, of the claims in this application.

Listing of Claims:

1. (Currently Amended) A method, comprising:
~~storing in a second~~ generating by a first apparatus which controls access to a radio communications network a shared secret ~~generated~~ at the ~~second~~ first apparatus and storing the shared secret in a memory of the first apparatus, wherein the stored secret is associated with an operational mode of the ~~second~~ first apparatus;

making the stored shared secret available at a ~~first~~ second apparatus ~~without~~ ~~contemporaneous user input~~;

receiving a signal from the second apparatus to establish communication with the first apparatus on the radio communications network, where the signal comprises a request for a required service from the first apparatus;

determining whether the first apparatus is in the operational mode where a user of the first apparatus does not want to be interrupted and whether the required service is associated with the stored shared secret; and

based on the determining, creating, ~~in the second apparatus, using the secret~~ a secret key for use in pairing to secure communication between them, where the secret key is created using an algorithm.

2. (Currently Amended) The method as claimed in claim 1, wherein ~~the secret~~ ~~is previously generated at the second apparatus by user input to the second~~ ~~apparatus~~ for the case it is determined that the first apparatus is in the operational

mode where the user of the first apparatus does not want to be interrupted and that the required service is associated with the stored shared secret, then automatically accessing the stored shared secret associated with the required service without contemporaneous user input, or else

prompting the user of the first apparatus to enter a shared secret associated with the requested service; and

where the algorithm uses one of the stored shared secret and the shared secret entered by the user as an input to the algorithm.

3.   (Currently Amended) The method as claimed in claim 1, ~~wherein the operational mode comprises a game mode~~ further comprising, based on at least the created secret key, establishing the communication with the second apparatus and providing the requested service to the second apparatus.

4.   (Currently Amended) The method as claimed in claim 1, wherein the ~~stored secret is associated with a service provided by the second apparatus~~ determined operational mode comprises a gaming mode.

5.   (Currently Amended) The method as claimed in claim 1, further comprising, ~~at the second apparatus, receiving a signal from the first apparatus; determining that the signal is associated with the operational mode of the second apparatus; and in response to the determining, automatically creating without user intervention, the secret key,~~ selecting the operational modes where the user of the first apparatus does not want to be interrupted.

6.   (Currently Amended) The method as claimed in claim 1, where ~~making the stored secret available at the first apparatus is without communication in the radio communications network~~ the required service comprises a gaming service.

7.   (Currently Amended) The method as claimed in claim 1, wherein making the stored shared secret available at the ~~first~~ second apparatus involves prompting a user input of the shared secret at the ~~first~~ second apparatus.

8.   (Currently Amended) The method as claimed in claim 1 ~~further comprising storing in the second apparatus an identifier of the first apparatus and an identifier of the second apparatus~~ where the shared secret comprises a secret PIN.

9.   (Currently Amended) The method as claimed in claim 1, wherein the algorithm creating the secret key uses a random number communicated between the first apparatus and the second apparatus.

10.   (Currently Amended) The method as claimed in claim 1, wherein the algorithm creating the secret key uses an identifier of one of the first apparatus and the second apparatus, communicated between the first apparatus and the second apparatus, in the creation of the secret key.

11.   (Currently Amended) The method as claimed in claim 1, further comprising: re-using the stored shared secret to join a third apparatus to ~~a~~ the radio communications network without contemporaneous user input of ~~a~~ the shared secret at the ~~second~~ first apparatus, comprising: making the stored shared secret available at the third apparatus; and

creating in the ~~second~~ first apparatus, using the shared secret, a secret key; and making the secret key available to the third apparatus for use in pairing the third apparatus and ~~second~~ the first apparatus to secure communication between them.

12.   (Currently Amended) A method, comprising:

storing, in a ~~second~~ memory of a second apparatus ~~which controls access to a radio communications network~~ a ~~generated~~ shared secret ~~at the second apparatus~~,

5

wherein the stored <u>shared</u> secret is associated with an operational mode of the second apparatus; ~~making the stored secret available to each of at least one or more first apparatus; and creating in the second apparatus, using the secret, at least one secret key for use in pairing the one or more first apparatus and the second apparatus to secure communication between them~~

<u>sending a signal to a first apparatus to establish communication with the first apparatus, where the signal comprises a request for a required service from the first apparatus;</u>

<u>determining whether the second apparatus is in an operational mode where a user of the second apparatus does not want to be interrupted and whether the required service is associated with the stored shared secret; and</u>

<u>based on the determining, creating a secret key for use in establishing the communication with the first apparatus, where the secret key is created using an algorithm.</u>

13.   (Currently amended) The method as claimed in claim 12, wherein ~~the step of creating at least one secret key comprises: creating a plurality of secret keys distributed across the first apparatus by creating a different secret key at each of the at least one or more first apparatus; and creating an identical plurality of secret keys at the second apparatus~~

<u>for the case it is determined that the second apparatus is in an operational mode where the user of the second apparatus does not want to be interrupted and that the requested required service is associated with the stored secret, then automatically accessing the stored shared secret associated with the requested service without contemporaneous user input, or else</u>

<u>prompting the user of the apparatus to enter a shared secret associated with the requested service; and</u>

where the algorithm uses one of the stored shared secret and the shared
secret entered by the user as an input to the algorithm.

14. (Currently Amended) An apparatus comprising:

~~a user interface configured to generate a secret by user input;~~
a memory ~~configured to store~~ storing a ~~generated~~ shared secret for use in securing
communications in a radio communications network comprising the apparatus and one or
more additional apparatus, wherein the stored shared secret is associated with an operational
mode of the apparatus;

a radio transceiver configured to communicate in the network and to receive a signal from the
one or more additional apparatus to establish communication with the apparatus on the
communications network, where the signal comprises a request for a required service from
the apparatus;

at least one processor configured to determine whether the apparatus is in an operational
mode where a user of the apparatus does not want to be interrupted and whether the required
service is associated with the stored shared secret; and

a the at least one processor configured, based on the determining, to ~~access the secret stored
in the memory and to create, using the accessed secret,~~ create a secret key for use in pairing
the apparatus and the one or more additional apparatus to secure communication between
them, where the secret key is created using an algorithm.

15. (Currently Amended) The apparatus as claimed in claim 14, comprising a
user interface; and

wherein ~~the user interface is configured to generate the stored secret by user input~~

7

for the case where the at least one processor determines that the apparatus is in the operational mode where the user of the apparatus does not want to be interrupted and that the required service is associated with the stored secret, the at least one processor configure to automatically access the stored secret associated with the required service without contemporaneous user input, or else

the user interface is configured, for the case it is determined one of the apparatus is not in the operational mode and the required service is not associated with the stored secret, to prompt the user of the apparatus to enter a secret associated with the requested service; and

where the algorithm uses one of the stored secret and the secret entered by the user as an input to the algorithm.

16.   (Previously Presented) The apparatus as claimed in claim 14, wherein the operational mode comprises a game mode.

17.   (Currently Amended) The apparatus as claimed in claim 14, wherein the stored secret is associated with a service provided by the apparatus required service comprises a gaming service.

18.   (Currently Amended) The apparatus as claimed in claim 14, wherein the radio transceiver is configured to receive a signal from any one of one or more additional apparatus; the processor is configured to determine that the signal is associated with an operational mode of the apparatus; and comprising the at least one processor is configured, in response to the determining, to access the secret in the memory to create the secret key without user intervention.

19.   (Currently Amended) The apparatus as claimed in claim 18 claim 14, wherein the at least one processor is operable configured to automatically create the secret key in response to

the received signal.

20.   (Currently Amended) The apparatus as claimed in ~~claim 18~~ claim 14, wherein the stored shared secret is independent of an origin of the received signal.

21.   (Currently Amended) The apparatus as claimed in ~~claim 18~~ claim 14, wherein the secret key is dependent upon an origin of the received signal.

22.   (Currently Amended) The apparatus as claimed in ~~claim 18~~ claim 14, wherein ~~the received signal is a request and~~ the secret key is dependent upon content of the received request.

23.   (Currently Amended) The apparatus as claimed in claim 22, wherein the request includes a random value used with at least the stored shared secret to create the secret key.

24.   (Currently Amended) The apparatus as claimed in claim 14, wherein the at least one processor is configured, in a first mode, to obtain a secret by accessing the shared secret stored in the memory, is configured, in a second mode, to obtain a shared secret by enabling user input of data, and is configured, in the first mode and in the second mode, to create, using the obtained shared secret, the secret key for use in pairing the apparatus and the one or more additional apparatus to secure communication between them.

25.   (Previously Presented) The apparatus as claimed in claim 24, wherein the first mode is an interactive gaming mode and second mode is an idle mode.

26.   (Currently Amended) The apparatus as claimed in claim 14, wherein the memory stores an apparatus identifier for use with at least the stored shared secret to create the secret key.

27.   (Currently Amended) The apparatus as claimed in ~~claim 14~~ claim 15, further comprising ~~a~~ the user ~~input apparatus~~ interface is configured to program the value of the

stored <u>shared</u> secret.

28.   (Previously Presented) The apparatus as claimed in claim 14, wherein the secret key is for use in securing all communications in the network.

29.   (Currently Amended) The ~~apparatus as claimed in claim 14, wherein the memory is configured to store a secret for use in securing communications in the network between the apparatus and a first additional apparatus and between the apparatus and a second additional apparatus, the processor is configured to access the secret in the memory and to create, using the secret, a first secret key in common with the first additional apparatus for use in pairing the apparatus and the first additional apparatus to secure securing communication between the apparatus and the first additional apparatus and a second secret key in common with the second additional apparatus for use in pairing the apparatus and the second additional apparatus to secure communication between the apparatus and the second additional apparatus~~ <u>memory embodying instructions executable by a processor of claim 35, wherein for the case it is determined that the first apparatus is in the operational mode where the user of the first apparatus does not want to be interrupted and that the required service is associated with the stored shared secret, then automatically accessing the stored shared secret associated with the required service without contemporaneous user input, or else</u>

<u>prompting the user of the first apparatus to enter a shared secret associated with the requested service; and</u>

<u>where the algorithm uses one of the stored shared secret and the shared secret entered by the user as an input to the algorithm.</u>

30.   (Currently Amended) The apparatus as claimed in claim 14, further comprising a user interface configured to enable data entry, wherein when the apparatus participates in a

different network controlled by a different apparatus the user interface is configured to enter a shared secret stored at the different apparatus and the at least one processor is ~~operable~~ configured to create, using the entered shared secret, a secret key for securing communication.

31-33. (Canceled)

34. (Currently Amended)   An apparatus comprising:
~~means for storing in a second apparatus which controls access to a radio communications network a secret generated at the second apparatus, wherein the stored secret is associated with an operational mode of the second apparatus;~~
~~means for making the stored secret available at a first apparatus without contemporaneous user input; and~~
~~means for creating in the second apparatus, using the secret, a secret key for use in pairing the first apparatus and the second apparatus to secure communication between them~~
a radio transceiver configured to communication on a radio communications network;

a memory storing a shared secret for use in securing communications in the radio communications network, wherein the stored shared secret is associated with an operational mode of the apparatus;

the radio transceiver configured to send a signal to another apparatus to establish communication with the another apparatus on the communications network, where the signal comprises a request for a required service from the another apparatus;

at least one processor configured to determine whether the apparatus is in an operational mode where a user of the apparatus does not want to be interrupted and whether the required service is associated with the stored shared secret; and

the processor configured, based on the determining, to create a secret key for use in pairing

over the communications network the apparatus and the another apparatus to secure communication between them, where the secret key is created using an algorithm.

35. (Currently Amended)   A memory embodying a program of computer readable instructions that when executed by a processor perform actions directed to securing communication between a first and second apparatus, the actions comprising:

~~storing in the second apparatus which controls access to a radio communications network a secret generated at the second apparatus, wherein the stored secret is associated with an operational mode of the second apparatus;~~

~~making the stored secret available at the first apparatus without contemporaneous user input; and~~

~~creating in the second apparatus, using the secret, a secret key for use in pairing the first apparatus and the second apparatus to secure communication between them~~

generating a shared secret at the first apparatus which controls access to a radio communications network and storing the shared secret in a memory of the first apparatus, wherein the stored shared secret is associated with an operational mode of the first apparatus;

making the stored shared secret available the second apparatus;

receiving a signal from the second apparatus to establish communication with the first apparatus on the radio communications network, where the signal comprises a request for a required service from the first apparatus;

determining whether the first apparatus is in an operational mode where a user of the first apparatus does not want to be interrupted and whether the required service is associated with the stored shared secret;

and

creating a secret key for use in establishing the communication with the second apparatus,

where the secret key is created using an algorithm.

36. (Previously Presented) The memory embodying instructions executable by a processor of claim 35, wherein the operational mode comprises a game mode.

37. (Currently Amended) The ~~memory embodying instructions executable by a processor of claim 35 comprising,~~ apparatus as claimed in claim 34 comprising

a user interface; and

wherein for the case it is determined that the apparatus is in an operational mode where the user of the apparatus does not want to be interrupted and that the required service is associated with the stored shared secret, the at least one processor is configured to automatically access the stored shared secret associated with the required service without contemporaneous user input, or else

the user interface is configured, for the case it is determined one of the apparatus is not in the operational mode and the required service is not associated with the stored secret, to prompt the user of the apparatus to enter a shared secret associated with the requested service; and

where the algorithm uses one of the stored shared secret and the shared secret entered by the user as an input to the algorithm

~~receiving a signal, at the second apparatus, from the first apparatus;~~

~~determining that the signal is associated with the operational mode of the second apparatus; and~~

~~in response to the determining, automatically creating, without user intervention, the secret key.~~